

WHAT IS CLAIMED IS:

1. A method for reducing the number of exploitable vulnerabilities in a software

application, said method comprising:

creating a vulnerability knowledge database comprising one or more classes of known software vulnerabilities;

applying a code parser to the software application to generate an abstract syntax tree;

comparing the abstract syntax tree and the classes of known software vulnerabilities to identify a set of potential exploitable software vulnerabilities; and

performing a static analysis of the set of potential exploitable software vulnerabilities wherein the static analysis is flow sensitive analysis of a list of constraints, and wherein the results of the static analysis comprise a set of exploitable software vulnerabilities.